

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

370

Vragen van het lid **Mutluer** (GroenLinks-PvdA) aan de Minister van Justitie en Veiligheid over *geld terugvorderen van fraudeurs door slachtoffers van online oplichting* (ingezonden 25 september 2024).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 23 oktober 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 317.

Vraag 1

Bent u bekend met de uitzending van Pointer van 21 september 2024 over slachtoffers van online oplichting die geld terugvorderen van fraudeurs?¹

Antwoord 1

Ja, ik ben met deze uitzending bekend.

Vraag 2

Herkent u zich in de conclusie van Pointer dat er te weinig gebruik wordt gemaakt van de regeling procedure begunstigde NAW-gegevens bij niet-bancaire fraude (PNBF)?

Antwoord 2

Met de Procedure non-bancaire fraude (PNBF) helpen Nederlandse betaaldienstverleners hun rekeninghouders die slachtoffer zijn geworden van oplichting en die in verband met die fraude geld hebben overgeboekt. Het primaire doel van de procedure is dat de betaler, in dit geval het slachtoffer van online fraude, in staat wordt gesteld om zijn geld terug te krijgen van de ontvanger. De NAW-gegevens van de ontvanger worden daarom alleen onder strikte voorwaarden verstrekt aan het slachtoffer. Slachtoffers kunnen daarmee een civiele rechtsprocedure starten om het overgemaakte geld terug te vorderen. Uit contact van banken met slachtoffers blijkt dat slachtoffers hiertoe besluiten op basis van de door hen ingeschatte slagingskans en kosten van een gerechtelijke procedure ten opzichte van het schadebedrag. Een belangrijk onderdeel van de PNBF is dat de betaaldienstverlener van de betaler eerst aan de ontvanger verzoekt om het geld terug te boeken.

¹ Pointer, 21 september Van klik naar klacht: slachtoffers van oplichting vorderen geld terug van fraudeur (pointer.kro-ncrv.nl/van-klik-naar-klacht-slachtoffers-van-oplichting-vorderen-geld-terug-van-fraudeur).

Wanneer dit succesvol is, is de inzet van een civiele rechtsprocedure niet meer nodig. Het terugvorderen van geld via een rechter, een deurwaarder of andere bemiddelaar moet daarom worden gezien als een tweede poging om de ontvanger tot terugbetaling over te laten gaan.

Bemiddelingskantoren kunnen de PNBF niet aanvragen, dat kan alleen de rekeninghouder zelf doen bij diens eigen bank. De bemiddelingskantoren gaan aan de slag nadat de PNBF volledig is afgerond. Daardoor hebben die kantoren, waar Pointer voornamelijk de uitzending op baseert, geen volledig beeld van het gebruik van de PNBF. Betaaldienstverleners bevestigen dat de PNBF door gedupeerde klanten gebruikt wordt, maar spreken zich niet uit over aantallen. Het is gezien bovenstaande een te voorbarige conclusie om te zeggen dat de PNBF niet zou werken of onvoldoende gebruikt wordt.

Vraag 3

Kunt u cijfers aanleveren van het aantal mensen dat sinds 1 januari 2021 een beroep heeft gedaan op de regeling PNBF en dat daadwerkelijk geld heeft teruggekregen van fraudeurs via een deurwaarder? Zo ja, kunt u deze cijfers delen? Zo nee, wat gaat u doen om deze cijfers boven tafel te krijgen?

Antwoord 3

De PNBF is geen regeling van de overheid, maar een regeling van de Nederlandse Betaaldienstverleners. Banken houden voor de PNBF geen centrale registratie bij. Voor de beantwoording van de vraag om een indicatie hoeveel verzoeken er zijn gedaan sinds 2021 kan geen antwoord worden gegeven binnen de gevraagde beantwoordingstermijn. Wel zeg ik u toe dat mijn ministerie met de Nederlandse Vereniging van Banken en Betaalvereniging Nederland in gesprek zal gaan om te bezien of het mogelijk is om dergelijke gegevens boven water te krijgen.

Vraag 4

Wordt door Nederlandse banken en de Betaalvereniging Nederland geregistreerd hoeveel mensen gebruik maken van deze regeling en hoe vaak binnen drie weken geld is overgemaakt door de oplichter nadat die is benaderd door de bank? Kunt u dit uitgebreid en cijfermatig beantwoorden? Zo nee, bent u bereid om daar afspraken over te maken met banken en de Betaalvereniging Nederland zodat de effectiviteit van de regeling beter gemeten kan worden?

Antwoord 4

Zoals vermeld in mijn antwoord op vraag 3, is de regeling een private regeling van de banken en niet van de overheid. Betaaldienstverleners geven de NAW-gegevens pas op het moment dat aan de voorwaarden hiertoe is voldaan én duidelijk is dat de ontvanger het bedrag nog niet volledig heeft teruggeboekt op de uiterste betaaldatum die de betaaldienstverlener eerder vermeldde aan zowel de betaler als aan de ontvanger. Het verschil tussen het aantal aanvragen van de PNBF en het aantal NAW-verstrekingen in het kader van deze procedure kan verschillende oorzaken hebben, bijvoorbeeld: voldeed de aanvraag om de PNBF te starten aan de voorwaarden, wil de betaler de NAW-gegevens wel ontvangen, of is er berusting bij het slachtoffer dat het terugbetaalverzoek van de betaaldienstverlener niet tot terugbetaling leidt? Zoals ik in het antwoord op vraag 3 heb toegelicht, er is geen centrale registratie voorhanden.

Vraag 5

Worden slachtoffers van online fraude standaard op deze regeling gewezen? Zo ja, hoe vaak is dat gemiddeld jaarlijks sinds 2021 gebeurd door de politie, Slachtofferhulp, Helpdeksfraude, Consumentenbond en banken? Deelt u de mening dat dit staande praktijk zou moeten worden? Hoe gaat u daarvoor zorgdragen?

Antwoord 5

Ja, banken hebben mij laten weten dat zij in de regel iedere klant die daarvoor in aanmerking komt op de regeling van de PNBF wijzen. Slachtoffers die (online) aangifte doen bij de politie ontvangen via de statusupdate van hun aangifte standaard informatie over deze regeling en worden doorverwezen naar de Betaalvereniging Nederland en Slachtofferhulp voor

meer informatie en uitleg over de procedure. Ook de Fraudehelpdesk bevestigt dat melders standaard worden gewezen op de mogelijkheid van de PNBf.

Vraag 6

Klopt het dat slachtoffers in geval van online aangifte niet automatisch een bericht krijgen van de politie dat van deze regeling gebruik kan worden gemaakt? Zo ja, hoe gaat u hier wel voor zorgen?

Antwoord 6

Nee dit klopt niet. Slachtoffers worden in het geval van online aangifte wel automatisch geïnformeerd over de mogelijkheden van de regeling PNBf. Ik verwijs u naar mijn antwoord op vraag 5.

Vraag 7

Hoe wilt u ervoor zorgen dat de regeling PNBf meer bekendheid geniet?

Antwoord 7

Op dit moment worden slachtoffers van online fraude actief gewezen op de mogelijkheden van de regeling PNBf door banken, politie en de meldpunten. Het is aan de banken om hun gedupeerde rekeninghouders te helpen en ook actief door te verwijzen naar de politie en de PNBf. Het is niet aan de overheid om de communicatie over particuliere schaderegelingen zoals de PNBf over te nemen, wel stimuleert mijn ministerie de ketenpartijen binnen de integrale aanpak online fraude om slachtoffers actief door te verwijzen. Met de meldpunten worden afspraken gemaakt over de warme doorverwijzing naar gespecialiseerde hulp en ondersteuning van slachtoffers. Het belang van deze vuistregels is dat slachtoffers snel geholpen kunnen worden.

Vraag 8

Wanneer wordt de regeling geëvalueerd? Bent u bereid om daar afspraken over te maken met banken en de Betaalvereniging Nederland?

Antwoord 8

Zoals toelicht in mijn antwoord op vraag 3, is de procedure van de betaaldienstverleners een particuliere regeling. Deze regeling bestaat in aanvulling op de mogelijkheid die het Wetboek van Strafvordering, boek 1, artikel 126nc biedt.² Leden van Betaalvereniging Nederland bieden deze procedure belangeloos en kosteloos aan. Zoals toegezegd in mijn antwoord op vraag 3, zal ik in gesprek gaan met de Betaalvereniging Nederland, daar zal ik ook aandacht vragen voor het evalueren van de regeling. Of en op welke wijze de Betaalvereniging en banken daar opvolging aan willen geven is verder aan hen.

Vraag 9

Hoe staat het met de uitrol van de pilot van de politie om fraude bij online handel tegen te gaan waarin 87 procent van de 211 slachtoffers die meededen een resultaat hadden?³

Antwoord 9

De politie heeft een kleinschalige pilot uitgevoerd waarbij het ging om fraudezaken waarbij iemand iets online had besteld en vervolgens geen product ontving. De fraudegevallen werden direct na aangifte met instemming van de slachtoffers behandeld door de Landelijke Associatie van Gerechtsdeurwaarders (LAVG), en de Service Organisatie Directe Aansprakelijkstelling (SODA). Die organisaties stelden vervolgens de verdachten namens het slachtoffer aansprakelijk. Zo konden slachtoffers via een civiele procedure hun geld terugkrijgen. Op deze manier wilde de politie zorgen voor een betekenisvolle afhandeling voor slachtoffers en tegelijkertijd (mogelijke) daders ontmoedigen. Binnen deze pilot had niet 87, maar 47 procent van de 211 slachtoffers een resultaat. Momenteel voert de politie in samenwerking

² Dit artikel heeft betrekking op het vorderen van gegevens binnen het strafrecht.

³ Politie, 2 april 2022, Online opgelicht? Toch je geld terug (www.politie.nl/nieuws/2022/april/1/online-opgelicht-toch-je-geld-terug.html).

met het Openbaar Ministerie een pilot uit die is uitgerold in drie eenheden, namelijk de eenheid Noord-Holland, de eenheid Midden-Nederland en de eenheid Limburg. Deze pilot staat los van de PNBf procedure. Voorts doet de Haagse Hogeschool op dit moment onderzoek naar een toekomstbestendige civielrechtelijke afdoening van online fraude. Daarbij wordt gekeken naar drie verschillende routes: 1. Via de betaaldienstverlener (o.a. de PNBf-procedure); 2. Via de civiele rechtsvertegenwoordiger; en 3. Via de politie.

Als het gaat om de pilot directe aansprakelijkheid wordt nader onderzocht of de doelen van de pilot daadwerkelijk worden behaald. Het onderzoek bestaat uit 7 deelonderzoeken. Deelonderzoek 1 en 4 zijn opgeleverd en openbaar.⁴ Voor de zomer van 2025 zullen de eerste zes deelonderzoeken naar verwachting zijn opgeleverd en zal de balans kunnen worden opgemaakt door mijn ministerie, de politie en andere betrokken partijen.

Vraag 10

Kan de regeling ook worden uitgebreid naar payment providers als Mollie, Adyen en Paypal? Zo nee, waarom niet? Zo ja, op welke wijze, onder welke voorwaarden en binnen welk termijn?

Antwoord 10

Het is aan de betaaldienstverleners om deze particuliere regeling uit te breiden.

Vraag 11

Kunt u aangeven wat er is gebeurd met de projecten die zijn beloofd in de Kamerbrief over de voortgang samenwerking banken en politie bij de aanpak van internetoplichting en daarbij ook specifiek ingaan op de onderstaande vragen?⁵

Antwoord 11

In 2023 is de integrale aanpak online fraude met private en publieke partijen van start gegaan. Vanuit deze aanpak zijn enkele van de activiteiten zoals benoemd in de Kamerbrief Integrale aanpak online fraude in gang gezet.⁶ Zo hebben de banken de PNBf-regeling opgesteld en is de politie samen met het Openbaar Ministerie begonnen met de pilot directe aansprakelijkheid van fraude bij online handel. Daarnaast kunnen slachtoffers via de checkfunctie op politie.nl relevante informatie ophalen en wordt er in preventiecampagnes van onder andere de banken en politie voorlichting gegeven om te voorkomen dat burgers zich laten gebruiken als geldezel.

Vraag 12

Wat heeft het onderzoek naar de mogelijkheden voor slachtoffers van internetoplichting om hun schade gecontroleerd te laten verhalen op de fraudeur en naar ondersteuning hierbij door banken en politie opgeleverd?

Antwoord 12

Zoals in mijn antwoord op vraag 9 is toegelicht, is de pilot directe aansprakelijkheid verder uitgerold. Ook loopt er nog onderzoek door de Haagse Hogeschool in opdracht van de politie naar de ervaringen van slachtoffers bij het verhalen van schade. Dit is één van de zeven deelonderzoeken. De uitkomsten zal ik betrekken bij de beleidsontwikkeling.

Vraag 13

Is er daadwerkelijk gezorgd voor betere detectie van fraude in het transactie-verkeer van banken, onder andere door het delen van modus operandi van criminelen tussen politie en banken t.b.v. een slimme monitoring van dat transactieverkeer? Zo ja, waar blijkt dat uit?

⁴ Civielrechtelijke afdoening van online fraude <https://www.dehaagsehogeschool.nl/onderzoek/kenniscentra/civielrechtelijke-afdoening-van-online-fraude>.

⁵ Kamerstuk 28 684, nr. 638

⁶ Kamerstuk 29 911, nr. 393.

Antwoord 13

Banken werken continu aan het verbeteren van hun fraudedetectie. Een van de signalen die hiervoor wordt gebruikt, zijn de meldingen van het Landelijk Meldpunt Internetoplichting wanneer er (minimaal) drie keer een aangifte is gedaan waarbij een rekeningnummer van een van de Nederlandse banken is betrokken. Deze informatie wordt actief gebruikt om onderzoek te doen naar de rekening van een klant. Daarnaast werken de banken en de politie samen in de Electronic Crime Taskforce en wisselen met elkaar modus operandi uit, zodat de opsporing gericht wordt ingezet en om te komen tot vervolging van de betrokken criminelen.

Vraag 14

Is er gezamenlijk wetenschappelijk onderzoek gedaan door banken en politie in samenwerking met de Universiteit Twente naar de factoren die leiden tot slachtofferschap, het vergroten van de meldingsbereidheid door slachtoffers en handvatten voor het voorkomen van fraude? Zo ja wat waren de belangrijkste conclusies, en hoe zijn die opgevolgd?

Antwoord 14

Ja, in 2022 is dit onderzoek genaamd «Victimisatie in Nederland» gepubliceerd. Het onderzoek is uitgevoerd door de Universiteit Twente in gezamenlijke opdracht en met financiering van Verzekeraars, de NVB, ICS en de politie. De belangrijkste conclusies (voor het peiljaar 2020) zijn dat de totale schade door de onderzoekers werd geschat op 2,75 miljard, dat aankoopfraude de meest voorkomende vorm was, dat fraude bij de politie en andere private partijen niet vaak gemeld werd en dat het aantal slachtoffers zou kunnen dalen als burgers beter op de hoogte zijn van de modus operandi van fraudeurs. Deze bevindingen worden betrokken bij de integrale aanpak online fraude. Dit licht ik nader toe in antwoord op vraag 20.

Vraag 15

Welke acties zijn ondernomen om de vindbaarheid, het gebruik en de effectiviteit van de checkfunctie op politie.nl te verbeteren? Is dat effectief gebleken? Zo ja, waaruit blijkt dat?

Antwoord 15

Verschillende publieke en private organisaties, zoals de consumentenorganisaties en financiële instellingen, verstrekken informatie over deze checkfunctie. In 2024 hebben er tot eind september naar schatting 210.000 burgers gebruik gemaakt van deze checkfunctie.

Vraag 16

Wat is de uitkomst van de betere detectie van geldezels op basis van profielen en indicatoren die zou plaatsvinden?

Antwoord 16

Het Centrum voor Criminaliteitsbestrijding en Veiligheid (CCV) zet op verzoek van het Ministerie van Justitie en Veiligheid vanuit de City Deal Lokale Weerbaarheid Cybercrime in op de lokale aanpak van geldezels. Dit gebeurt binnen vier pilots die worden uitgevoerd binnen Preventie met gezaggemeenten. In deze aanpak wordt zoveel mogelijk kennis gebundeld vanuit wetenschap en praktijk en wordt samenwerking gestimuleerd tussen partners zoals politie, Openbaar Ministerie, Zorg- en Veiligheidshuizen, onderwijs, jongerenwerk en andere lokale partners.

Vraag 17

Hoe heeft u de afgelopen tijd gezorgd voor het bewustmaken van doelgroepen om te voorkomen dat zij ten prooi vallen en geldezel worden? Hoe verklaart u dat het aantal geldezels is toegenomen?

Antwoord 17

Criminelen proberen op alle mogelijke manieren anoniem te blijven en verzinnen steeds weer nieuwe manieren om hun illegale geld te verstoppert. Het blijft van groot belang om de weerbaarheid van alle doelgroepen te vergroten, zowel offline (bijvoorbeeld op scholen) als online (via een social media campagne). Geldezels zonder criminele antecedenten worden ervan

doordrongen dat een misstap niet moet leiden tot verder crimineel gedrag. Hierbij wordt nagegaan wat hen ertoe leidde om als geldezels op te treden en wordt geprobeerd die oorzaak weg te nemen. Tot slot worden interventies ingezet voor de aanpak van geldezels met meerdere antecedenten, zoals stopgesprekken door politie en de inzet van een persoonsgerichte aanpak. De resultaten van de pilots van het CCV worden in het tweede kwartaal van 2025 verwacht. Aan de hand daarvan is de verwachting dat er een gevalideerde aanpak landelijk kan worden geïmplementeerd.

Vraag 18

Wat zijn de uitkomsten van het onderzoek naar de versterking van de gegevensdeling tussen de politie en de banken in het kader van de samenwerking binnen het Landelijk Meldpunt Internetoplichting?

Antwoord 18

Er is een samenwerking tussen het Landelijk Meldpunt Internetoplichting (LMIO) en de banken als het gaat om notificaties aan een bank wanneer er meerdere keren aangifte is gedaan tegen een rekeninghouder. Het LMIO heeft samen met Surepay onderzocht hoe de initiërende bank zijn rekeninghouder kan beschermen als die een transactie verricht waarbij de begunstigde rekeninghouder voorkomt in de database van het LMIO. Hiermee kan in een vroeg stadium fraude worden voorkomen, door een overboeking naar een frauduleuze bankrekening te voorkomen. De eerste resultaten lijken positief, met name voor overboekingen naar bankrekeningen in het buitenland. Er worden momenteel verkennende gesprekken gevoerd met meerdere banken om deze interventie op kleine schaal te testen.

Er zijn initiatieven genomen door een tweetal banken om proactief het LMIO te benaderen om slachtoffergegevens te verkrijgen zodat zij «bevroren» gelden op een rekening van een fraudeur, en afkomstig van fraude, terug te kunnen storten naar de bankrekening van het slachtoffer. Verder heeft één bank contact gezocht met het LMIO om actief malafide webwinkels, dan wel als er een verdenking is dat het een webwinkel malafide is, te melden aan het LMIO, zodat door de politie onderzoek gedaan kan worden en de webwinkel offline kan worden gehaald.

Vraag 19

Welke acties zijn ondernomen ten aanzien van de inrichting en uitvoering van gezamenlijke communicatie ten behoeve van preventie en met welke uitkomst?

Antwoord 19

In 2023 is mijn ministerie samen met de Ministeries van Financiën en Economische Zaken en enkele publieke en private partners, waaronder banken, gestart met de integrale aanpak online fraude. Binnen deze aanpak is preventie één van de belangrijkste pijlers. Gezamenlijk wordt er gezorgd voor een communicatiestrategie waarbij er zoveel mogelijk kansen worden benut om burgers en bedrijven weerbaarder te maken tegen online fraude en om (herhaald) slachtofferschap te voorkomen. Zo wordt er onder andere voor gezorgd dat burgers en bedrijven worden voorgelicht op relevante beurzen, wordt er gewerkt aan een zelfhulptool voor slachtoffers, worden er folders en online informatie ontwikkeld en wordt ervoor gezorgd dat politie, banken en meldpunten slachtoffers zo goed mogelijk informeren en voorlichten over modus operandi van online fraudeurs. De Fraudehulpdesk voert in de decembermaand de voorlichtingscampagne «Eerst checken dan bestellen» uit. En scholieren.com start een campagne om jongeren meer bewust te maken van veilig internetgedrag.

Vraag 20

Welke acties zijn ondernomen om de samenwerking, tussen banken, Collecting Payment Service Providers, online handelsplatforms, de politie en het Openbaar Ministerie te versterken en hierbij te werken aan de ontwikkeling van innovatieve wijzen om nog meer gezamenlijk op te treden bij de

bestrijding van Internetoplichting en ondersteuning van fraudeslachtoffers, zoals uw voorganger beloofde in de Kamerbrief?⁷

Antwoord 20

Deze genoemde partijen, behalve de payment service providers, zijn betrokken bij de integrale aanpak online fraude. Hierbij wordt onder andere onderzoek gedaan naar technische barrières en interventies. Technologie maakt veel mogelijk, maar partijen geven ook aan dat zij ervaren dat de mogelijkheden worden beperkt door kaders voor gegevensdeling. Daarom wordt binnen de integrale aanpak ook de mogelijkheden voor gegevensdeling uitgewerkt en bezien of hier wetgeving nodig is om de gewenste interventies en innovatie meer ruimte te kunnen bieden.

Vraag 21

Kunt u deze vragen voorafgaand aan het commissiedebat over cybercrime in oktober beantwoorden?

Antwoord 21

Ja.

⁷ Kamerstuk 28 684, nr. 638